Comment « reguler » la protection des données ? Réflexions sur l'internormativité

Poullet, Yves

Published in:
Mélanges Paul Delnoy

Publication date:
2005

Document Version
le PDF de l'éditeur

COMMENT « RÉGULER » LA PROTECTION DES DONNÉES ? RÉFLEXIONS SUR L'INTERNORMATIVITÉ

PAR

Yves POULLET

Doyen de la Faculté de droit des Facultés universitaires Notre-Dame de la Paix
Professeur à la Faculté de droit de l'Université de Liège
Directeur du CRID des Facultés universitaires Notre-Dame de la Paix

Paul DELNOY ne m'en voudra pas, à l'heure d'écrire ces quelques lignes, d'évoquer la pensée d'un de ses amis chers : Michel COIPEL.

L'évocation de cette amitié me fournit le prétexte du choix du sujet ici traité.

L'ami commun a souligné l'importance de l'internormativité définie comme les multiples formes de dialogue entre la normativité juridique et les autres formes de normativités sociales, éthiques techniques ou imposées par le marché, normativité à l'œuvre dans la société [1].

Il m'apparaissait donc intéressant de prolonger, à l'occasion de cet hommage amical, les quelques réflexions sur la co-régulation proposées à l'occasion du *Liber Amicorum « Michel Coipel »* [2] en les appliquant à la matière que la Faculté de Droit me donne le plaisir d'enseigner à Liège : la protection de la vie privée et la société de l'information.

[1] M. COIPEL, « Quelques réflexions sur le droit et ses rapports avec d'autres régulations de la vie sociale », in *Gouvernance de la société de l'information*, Cahier du Crid, n° 22, Bruylant, Bruxelles, 2002, p. 43-76.

[2] Y. POULLET, « Technologies de l'information et de la « co-régulation » : une nouvelle approche », in *Liber Amicorum M. Coipel*, Kluwer, 2004, p. 167-188.

La société de l'information remet en cause les fondements même de l'ordre juridique et nécessite donc de repenser les « modes de production du droit ». Elle efface les frontières, multiplie les acteurs et introduit au cœur de son fonctionnement le fait « technologique ».

La remise en cause de l'État comme régulateur, même si elle n'est pas propre à ce seul domaine, y est plus patente encore. On rappelle volontiers à cet égard la « Déclaration d'indépendance du Cyberespace » de J.P. BARLOW[3] : « Gouvernements du monde industriel (...), je déclare l'espace social que nous construisons naturellement indépendant des tyrannies que vous cherchez à nous imposer. Vos définitions légales (...) ne s'appliquent pas à nous ». Ainsi, « si, écrit Fr. OST[4], hier, encore, l'œuvre législative était créditée du double postulat de la rationalité et de la souveraineté (la loi était censée exprimer les exigences de la raison et ses volontés avaient à s'appliquer sans détour ni discussion), aujourd'hui l'infaillibilité et l'autorité du législateur ne font plus l'objet que d'une présomption simple, quand elles ne sont pas carrément récusées ».

La régulation de la société de l'information ne peut être le fait unilatéral de l'État. Deux thèses toutes récentes, l'une française[5], l'autre suisse[6] ont largement démontré tout l'intérêt en la matière d'une multi régulation tant d'acteurs publics que privés. « En d'autres termes, écrit AMBLARD[7], la régulation de l'Internet se fonde par essence sur une approche pluraliste, c'est-à-dire sur des multiples formes de normes. L'Internet se régule donc par l'interaction des différentes activités normatives entre les législateurs nationaux, les juges, les instances de régulation sur l'Internet et les acteurs de l'Internet. » S'il est difficile de nier la présence du droit étatique dans le cyberespace, on voit poindre deux autres modèles de régulation : celle de l'autorégulation « dont la forme la plus poussée conçoit la souveraineté de l'utilisateur » et celle de la régulation par la technique « dont la forme la

[3] J.P. BARLOW, « Déclaration d'indépendance du Cyberespace », prononcé au Forum mondial de Davos, le 8 févr. 1996 et repris in *Thinking Locally, Acting Globally, Forum de discussion , Cyber-Rights*, 15 janv. 1996. Comp. Lessig, *Code and other Laws of Cyberspace*, New York, Basic Books, 1999,24 : « Le cyberespace ne peut pas être gouverné, il a une « habilité innée à résister à la régulation. C'est là sa nature, son essence, c'est ainsi que sont les choses (...) le cyberespace est un espace de non contrôle. »

[4] F. OST, « La régulation : des horloges et des nuages », in *Elaborer la loi aujourd'hui, mission impossible*, Publications FUSL, 1999, p. 12.

[5] Ph. AMBLARD, *Régulation de l'Internet - L'élaboration des règles de conduite par le dialogue inter-normatif*, Bruylant, Cahier du Crid, n° 24, 2004, 510 p.

[6] Th. SCHULTZ, *Réguler le commerce électronique par la résolution des litiges en ligne*, Thèse, Université de Genève, 2005, à paraître.

[7] Ph. AMBLARD, *op. cit.*, p. 105.

plus radicale érige les producteurs de standards techniques au rang de souverains »[8].

Cette diversité des modes de régulation est encouragée par le récent accord interinstitutionnel « Mieux légiférer » conclu le 16 décembre 2003 par le Parlement européen, le Conseil de l'Union européenne et la Commission des Communautés européennes[9].

Notre propos est à propos de la régulation de la protection des données dans le cyberespace de montrer dans un premier temps combien chacun des modes de régulation présente à la fois un intérêt mais également des limites au regard des critères de validité juridiques des normes en général : soit l'effectivité, la légitimité et la conformité[10]. Il s'agit donc de décrire séparément de ce point de vue, les trois modes de régulation. La réglementation publique traditionnellement confiée à l'œuvre législative est analysée essentiellement du point de vue de son *effectivité*[11]. Par « effectivité » d'une norme, on entend les mesures de garantie de respect de la norme, tant la manière dont elle est portée à la connaissance de ses destinataires, que les mesures de contrôle et de sanction. Les deux autres modes : l'autorégulation spontanée par les acteurs du marché et les solutions technologiques seront l'objet d'un examen plus complet tant des points de vue de leur *légitimité* et de leur *conformité* aux solutions réglementaires que de leur effectivité[12]. Le critère de légitimité renvoie à la qualité des auteurs et à la repré-

[8] Th. SCHULTZ, *op. cit.* Sur ces trois modes de régulation, lire en particulier, J. REIDENBERG, « Privacy Protection and the Interdependance of Law, Technology and Self-regulation », in *Variations sur le droit de la société de l'information*, Cahier du Crid, n° 20, Bruylant, 2002, p. 127 et s.

[9] Accord interinstitutionnel, publié au J.O.C.E., 31 déc. 2003, C 321/1.

[10] Sur ces trois critères de validité de la norme, lire nos réflexions in *Technologies de l'information et de la communication et co-régulation : une nouvelle approche ?, art. cité*, p. 169-171. On note que ces trois critères de validité sont présents dans l'accord européen cité note précédente. Ainsi, le point 17 de l'accord énonce : « La Commission veille à ce que le recours aux mécanismes de co-régulation et d'autorégulation soit toujours conforme au droit communautaire *(critère de conformité*)* et qu'il respecte des critères de transparence (publicité des accords notamment) et de représentativité des parties impliquées (*critère de légitimité).* Il doit en outre représenter une valeur ajoutée pour l'intérêt général (*critère de l'effectivité).* » (* les parenthèses en italiques sont des ajouts de l'auteur).

[11] À propos de l'effectivité en matière de protection des données, lire J.F. PERRIN, « La notion d'effectivité en droit européen, international et comparé de la protection des données », in *Mélanges offerts à P. Morand, Genève*, p. 197 et s. L'auteur écrit avec raison : « Une réglementation ne mérite le qualificatif d'« effective » que lorsqu'elle est mise en œuvre concrètement. Cette particularité essentielle s'observe sur les terrains et non dans les codes ».

[12] Sur ces trois critères fondés sur les écrits de SUMMERS (« Towards a better general Theory of legal Validity », *Rechtstheory*, 1985, 16, p. 65-77) et légèrement différents de ceux présentés par F. OST et M. VAN DE KERKHOVE (in *De la pyramide au réseau ?* Publications FUSL, 2002), lire nos réflexions in *Technologies de l'information et de la communication et « co-régulation » : une*

sentativité ou non des auteurs des normes non étatiques ; celui de la conformité au contenu de la régulation ainsi mise en place par rapport aux exigences du système juridique.

Le second temps décrit la façon dont la « loi », d'une part, renvoie à d'autres modes de régulation exprimée tant par des codes dits d'autorégulation que par des normes techniques, qu'elle les appelle voire les promeut et, d'autre part, envisage quelques tentatives de co-régulation en matière de protection des données. En d'autres termes, les suffixes » multi », « auto » et « co » constituent autant de variations d'un phénomène global, celui de la régulation [13] que l'État, à travers ces multiples modes, cherche à mobiliser, parfois à institutionnaliser au service d'une protection appropriée des protagonistes « tout en se modelant sur les usages et les contextes concrets dans lesquels se déroulent les activités de l'Internet » [14].

§ 1. Trois modes de régulation de la protection des données

A. La réglementation publique

Nos législations européennes de protection des données ont, à la suite des principes mis en place par la Convention n° 108 [15], limité le droit des entreprises et administrations à traiter des données à caractère personnel et consacré des droits nouveaux à la personne concernée.

Parmi ces droits nouveaux sur lesquels nous concentrerons notre propos, on cite le droit d'être informé de l'existence des traitements, le droit d'accès, le droit de correction et de recours.

nouvelle approche, op. cit., p. 170-171). Voir également celles de Schultz (*Thèse citée*), qui considère à tort selon nous que toute régulation normative est du droit au sens large suivant en cela les théories de sociologie du droit.

[13] Précisément à propos de la *Privacy*, les conclusions de Bennett et Raab (*The Governance of Privacy*, Ashgate, 2003, p. 96) : « Regulation does not only, or even principally, connote government command and control, involving legal requirements and their direct application, but embraces other tools as well. Thus, Majone takes self-regulation to be a mode of regulation, whilst Priest systematically elaborates several models of self-regulation as forms of regulation in which government's direct role varies ».

[14] P. Trudel, « Le droit de l'Internet au Canada », in *Internet et le Droit : Droit français, européen et comparé de l'Internet*, Actes du Colloques, Victoires, Paris, 2001, p. 160.

[15] Convention n° 108 du 28 janv. 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Il est intéressant de noter que nos législations modernes ont élargi ces droits à la mesure des défis rencontrés vu la complexité croissante des systèmes d'information. En particulier, l'accès aux données depuis la directive européenne 95/46/CE [16] ne se conçoit plus comme le seul accès au contenu des données, mais également à leur origine et surtout à la logique du traitement. La même directive 95/46 a créé le droit de ne pas être soumis à une décision prise sur la base d'un traitement automatisé de données, ce qui oblige au dialogue avec la personne concernée. Plus récemment la directive 2002/58/CE [17] a exigé le consentement pour l'envoi « à des fins de prospection directe » de communications électroniques.

Cette extension ne s'arrête pas à la reconnaissance de droits nouveaux pour la personne concernée mais affirme des obligations nouvelles à charge des responsables de traitement. À cet égard, on cite le récent *California Online Privacy Protection Act (OPPA)* [18] qui impose à tout prestataire de services Web qui collecte des données de créer une page web comprenant certaines informations [19].

L'effectivité de telles législations mérite quelques considérations.

Ainsi, si des droits nouveaux sont ainsi législativement consacrés, on s'aperçoit que leur exercice reste limité voire inexistant [20]. Les deux Eurobaromètres [21] publiés en 2003 par la Commission européenne en témoignent : 49 % des entreprises déclarent avoir reçu moins de 10 demandes d'accès en 2002 et 25 % aucune. On connaît la suite : « Pour la plupart des entreprises, constatent les auteurs de l'Eurobaromètre relatif à la perception

[16] Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel, *JOCE*, 23 nov. 1995, n° L 281, p. 31 et s.

[17] Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *JOCE*, 31 juil. 2001, n° L 201, p. 37 et s.

[18] Ce texte voté en 2003 est en application depuis le 1er juillet 2004. Il insère des sections nouvelles (22575-22579) dans le « Business and Professions Code » Californien.

[19] En particulier, on note outre les informations exigées traditionnellement par nos législations (l'identité du maître du fichier, le type de données collectées, les finalités d'utilisation), des données plus spécifiques au caractère éphémère des contenus des sites web, ainsi les procédures de modification et surtout la *Privacy Policy* du site et sa date de promulgation.

[20] À ce propos, les conclusions sévères et la dénonciation du « mythe de la protection légale », V. Sedaillan, » La loi informatique et Libertés : du mythe à la réalité », paper disponible sur le site http://www.europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/sedaillan_en.pdf.

[21] Cf. les deux Eurobaromètres publiés par la DG Marché intérieur et disponible sur le site : http://europa.eu.int/comm/justice_home/fsj/privacy Le premier (Eurobaromètre Spécial 196, sept. 2003) s'attache plus à l'opinion des citoyens européens, le second (Eurobaromètre Flash 147, sept. 2003), à celle des entreprises.

par les entreprises des législations de protection des données, la conformité à la loi n'est pas une priorité puisqu'elles reçoivent peu de plaintes ».

Sans doute, ceci est dû à la faible connaissance par les personnes concernées [22] tant de la question de la protection des données et de ses enjeux (70 % des Européens estiment que la protection des données est méconnue) que de l'existence des lois instituant cette protection (seuls 32 % ont entendu parler du droit d'accès, de rectification ou de suppression). Une autre raison est à notre avis la relative confiance des citoyens dans les mesures prises par leur pays même s'ils ignorent le contenu de ces mesures. On souligne l'effet pervers d'une intervention réglementaire qui déresponsabilise ceux qui devraient être les premiers acteurs de leur protection : les personnes concernées.

Au-delà, on note que l'effectivité des législations repose sur l'action des autorités de protection dont la création et les compétences sont consacrées par l'article 28 de la Directive 95/46/CE [23]. Avec leurs pouvoirs de recommandations, d'avis et d'injonctions, ces autorités administratives indépendantes apparaissent comme prolongeant par un droit que d'aucuns qualifient de souple, l'action réglementaire de l'État.

Ainsi, la loi n'est pas, par sa seule vertu, garantie d'effectivité et cherche à travers d'autres modes de régulation les moyens de son effectivité.

Sans doute, avec les interventions de l'autorité indépendante, reste-t-on dans la sphère publique, nous aurons l'occasion de montrer que le relais de l'effectivité légale peut être confié aux pouvoirs privés de l'autorégulation, que nous présentons maintenant.

[22] On ajoute que la lecture des lois de protection des données décourage le lecteur non initié voire l'avocat par son caractère abstrait et trop général. Comment le citoyen peut-il traduire des dispositions aussi absconses que celle suivant laquelle le responsable du fichier ne peut traiter des données de manière incompatible avec les finalités de la collecte lorsqu'il se trouve destinataire d'un e-mail envoyé par sa banque lui annonçant que sa prime d'assurance accident doit être augmentée vu les risques supplémentaires liés à la perte de son emploi, à ses mauvais placements boursiers ou simplement l'intérêt de contracter auprès d'elle une assurance moins chère que celle prise auprès d'un concurrent dont l'existence lui est révélée par un virement effectué ? Ce fait est relevé par nombre de citoyens : n'est-ce point un comble de constater cette difficulté de lecteur pour une loi, sensée apporter au citoyen protection et maîtrise de son environnement ?

[23] Ainsi chez nous, la Commission de protection de la vie privée, la Cnil en France, il Garante en Italie, etc. Sur le rôle « essentiel » de ces autorités administratives indépendantes dans la régulation de la société de l'information et en particulier de la protection des données, lire nos réflexions in *L'autorité de contrôle : Vues de Bruxelles, La protection des données à caractère personnel,* Rev. adm. publ., 89, IIAP, 1999, p. 81.

B. L'autorégulation

L'autorégulation, présentée comme le modèle alternatif à la régulation publique, peut être tentante. Les *Privacy Policy,* simple *commitments, codes of Practices ou Privacy Standards* [24] émanant des responsables de traitement, seuls ou encadrés, comme c'est le cas dans les *Safe Harbor Principles* [25] fleurissent. Ils présentent l'avantage pour la personne concernée de développer, dans un langage bien plus convivial que celui de la loi, des principes plus adaptés à la réalité des traitements d'une entreprise ou d'un secteur [26]. Ils reposent sur un engagement consciemment pris par un secteur ou une entreprise. Bref, l'auto-réglementation semble avoir l'avantage d'une plus grande effectivité [27].

À cet égard cependant, les reproches adressés à l'autorégulation sont connus : le premier est sans doute la question de la légitimité des multiples produits de cette auto-réglementation. Comme l'écrit WEBER [28], avec l'autorégulation, tout groupe pertinent n'est pas nécessairement impliqué ». Ainsi, on s'inquiète des codes de conduite imposés à l'internaute et non négociés avec ses représentants. Le second reproche est le manque de garan-

[24] Sur la directive entre ces trois types d'autorégulation, C.J. BENNETT et C.D. RAAB, *The gouvernance of Privacy, Ashgate,* 2003, p. 12 et s.

[25] Cf. à cet égard, la décision 2000/520/CE de la Commission conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la protection assurée par les principes de la sphère de sécurité et par les questions souvent posées y afférentes, publiées par le ministère du Commerce des Etats-Unis d' Amérique, JOCE, 25 août 2000, L 215, p. 7 et s. L'encadrement par les pouvoirs publics est assuré par le fait que les *Safe Harbor Principles* ont été négociés avec les pouvoirs publics et que les déclarations de conformité sont publiées sur le site officiel du *Department of Commerce.* Sur ces *Safe Harbor Principles* comme mode de corégulation, lire Y. POULLET, *Les « Safe Harbor Principles ; Une protection adéquate ?* Disponible sur : http://www.droit-technologie.org

[26] Sur cette meilleure adaptation de l'autorégulation aux besoins normatifs des protagonistes de la société de l'information, lire P. TRUDEL ET ALII, « *Droit du cyberespace* », Thémis, Montréal, 1997, Chap. 3, p. 12 et s.

[27] Pour un jugement très nuancé sur la situation aux Etats-Unis de l'effectivité des codes de conduite en matière de protection des données, lire K. JAMAL, M. MAIER et S. SUNDER, *Enforced Standards Versus Evolution by General Acceptance : A comparative Study of E-Commerce Privacy Disclosure and Practice in the U.S and the U.K.,* Joint Center, Working Paper, 03-08., July 2003.

[28] R.H. WEBER, *Regulatory models for the online World,* Zurich, Schulthess, 2002, p. 85. Sur ce même point, A. ROSSNAGEL, « Weltweites Internet-Globale Rechtsordnung », *Multimedia und Recht,* 2002, p. 69 et J. REIDENBERG, « L'instabilité et la concurrence des régimes réglementaires », in *Les incertitudes du droit,* E. MACKAAY (éd.), Montréal, Thémis, 1999, p. 133 et s. (à noter que l'auteur étend sa critique à la régulation technologique).

tie quant à l'effectivité de ce mode de régulation [29]. À cet égard, sans doute, faut-il distinguer suivant les différents types d'autorégulation signalés plus haut. Le *Privacy commitment* est un engagement de l'entreprise. Le *Privacy Code of practice* est défini à un niveau plus collectif, ainsi par un secteur professionnel. Les membres de ce « collectif » adhèrent aux principes et des sanctions, en cas de non-respect, peuvent être prévues par l'association qui a établi le code. Enfin, les « Standards » impliquent une procédure d'évaluation du respect de leur contenu par ceux qui déclarent les respecter. Cette procédure peut consister en une « certification » [30] de la conformité des traitements aux principes déclarés et la délivrance d'un label [31]. La définition de normes [32], dont le respect fait l'objet de vérifications et d'audit, est une autre procédure évoquée.

Le recours en cas de non-respect peut se voir facilité par la mise sur pied de *Alternative Dispute Resolution Mechanisms* [33] auxquels l'accès est facile,

[29] À ce propos, les recommandations de la *Federal Trade Commission* qui, en 2000, publiait un rapport (http://www.ftc.gov/reports/privacy2000/pdf) sur l'application des principes de *Fair Information* à la protection de la *privacy*. Cette instance concluait que les efforts d'autorégulation étaient insuffisants dans la pratique et recommandait le vote d' une législation fédérale adéquate, formulée en termes généraux et technologiquement neutre dans le cadre de laquelle l'autorégulation pourrait prendre sa place et obtenir une meilleure effectivité.

[30] Ainsi, celle de *Trust-e, du BBB Online, Privacy Programme, de Webtrust*, etc.

[31] Sur ces techniques de « labellisation », J.R. REIDENBERG, *Adapting Labels and Filters for Data Protection, Cybernews*, 1997, III, 6.

[32] On rappelle l'exemple canadien du « Model Code for the Protection of Personal Information », approuvé par le « Standards Council of Canada » en mars 1996. Plus récemment, les discussions relatives à l'adoption de normes en matière de sécurité et vie privée menées au sein de l'ISO ou du CEN. Sur tous ces développements, lire C.J. BENNETT et C.D. RAAB, *op. cit.*, pp. 121-137 et l'opinion 1/2002 en date du 30/5/2002, du Groupe de l'article 29 sur le rapport du CEN/ISS relatifs aux standards *Privacy* en Europe, http://europa.eu.int/comm/justice_home/fsj/privacy/docs10761/02/en/final

[33] À propos des ADR et de leur intérêt dans le domaine de la protection des données personnelles, lire la thèse de SCHULTZ, déjà citée. Ce dernier met en évidence la façon dont les divers modes d'autorégulation (code de conduite, label et ADR) peuvent se conjuguer pour fournir à la personne concernée une protection effective.
À noter que les *Safe Harbor Privacy Principles* font de la désignation d'un ADR un élément essentiel de la mise en œuvre (*Enforcement*) du système mis en place : « Pour protéger efficacement la vie privée, il convient de mettre au point des mécanismes permettant d'assurer le respect des principes de la « sphère de sécurité », de ménager un droit de recours aux personnes concernées par le non-respect des principes et de sanctionner les organisations. Ces mécanismes doivent comprendre au minimum : a) des systèmes de recours indépendants aisément accessibles et peu coûteux, permettant d'étudier et de résoudre toute plainte et tout litige ». Sur ces mécanismes, lire entre autres, M. SCHELLECKENS et L. VAN DER WEES, « ADR and ODR in E-Commerce », in *Trust in e-commerce*, Kluwer Law International, 2002, p. 271-300.

dont la compétence est évidente et par lesquels des solutions plus adaptées et constructives peuvent être trouvées.

Ainsi, le reproche du manque d'effectivité s'il apparaît évident vis-à-vis des formes « faibles » d'autorégulation, est à nuancer fortement vis-à-vis de ses formes plus avancées. Cependant, on déplorera la multiplication des labels et la difficulté d'en saisir la portée et parfois le contenu. L'autorégulation sauvage met à charge de la personne concernée le soin de vérifier la qualité de celle-ci [34].

Un deuxième reproche souligne les dangers du caractère « volontaire » de l'autorégulation. Sans doute, dira-t-on, l'absence de tout engagement ou la prise d'engagements à contenu faible amènera les personnes concernées à préférer l'entreprise concurrente qui s'est soumise à une autorégulation plus contraignante et à contenu plus protecteur. Une telle affirmation résiste peu à l'analyse lorsqu'on sait que parfois le choix n'existe point et qu'en toute hypothèse, le critère *Privacy Protection* n'est pas le plus déterminant dans le choix des personnes concernées.

La question de la conformité des solutions vis-à-vis des exigences de la loi soulève également difficulté. Elle rejoint le problème de la légitimité de leurs auteurs. Les « standards » définis dans le cadre de ses *Privacy Policies* sont souvent faibles dans la mesure où leur définition et leur contenu relèvent des seuls responsables de traitement, préoccupés de ne point trop augmenter leur charge [35]. Sans doute, la consultation des représentants des personnes concernées (les syndicats, les associations de consommateurs ou de libertés civiles) aurait permis d'améliorer grandement leur contenu.

[34] Sur ce point, D.J. SOLOVÉ, « Privacy and Power : Computer Databases and Metaphors for Information Privacy, 53 » *Stanford Law Review*(2001), 1393 et s. Cette crainte est confirmée par l'analyse réalisée pour la Commission européenne relative à l'application des *Safe Harbour Privacy Principles* déjà évoqués (À ce propos, lire en particulier les pages 105 et s. du rapport « *Safe Harbour Decision Implementation study* » (J. DHONT, M.V. PEREZ, Y. POULLET avec la collaboration de J. R. REIDENBERG et L. BYGRAEVE, disponible sur le site http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.htm))

[35] À ce propos, BENNETT ET RAAB (*op. cit.*, p. 136) notent l'intérêt de distinguer les codes de conduite couvrant l'ensemble d'un secteur, modèle répandu au Canada, Japon et Australie et ceux liés à la décision d'une entreprise comme c'est le cas aux États-Unis. Sur ce que SCHULTZ qualifie d'« insuffisance réflexive », lire ses réflexions (*op. cit.*) : « Le défaut majeur de l'autorégulation concerne à notre sens son insuffisance réflexive, c'est-à-dire l'équilibre toujours fragile de la représentativité de tous les intérêts des destinataires des normes produites. »

C. Les solutions technologiques

Les solutions technologiques[36] dites *Privacy Enhancing Technologies* (PETs) sont invoquées[37], avec de plus en plus d'insistance soit comme outil de protection des données à l'appui de solutions auto réglementaires comme le P3P[38], soit comme substitut aux autres modes de régulation comme la cryptographie[39].

On relève que ces solutions réglementaires peuvent être implémentées *au niveau de l'infrastructure,* ainsi on pourrait imaginer le blocage automatique des connexions vers des pays ne respectant pas les prescrits en matière de protection des données, *au niveau du responsable du traitement ou au niveau d'intermédiaires* comme l'utilisation de filtres par des serveurs spécialisés chargés de bloquer les « spams »[40] adressés par certains types d'entreprise ou, enfin, *au niveau des terminaux de la personne concernée* comme les outils de blocage de l'envoi et de réception de cookies ou permettant la négociation avec le responsable du traitement.

Les critiques de tels outils, dont on souligne l'effectivité[41], tiennent au contenu des règles qu'elles mettent en œuvre. Ces règles sont souvent négociées au sein de cercles d'experts, peu au courant des exigences de la protection des données ou plus sensibles aux besoins du monde professionnel qu'aux intérêts de la personne concernée. On dénonce également à propos des technologies dont la mise en œuvre dépend des personnes concernées elles-mêmes, le mythe de *l'User Empowerment*[42]. Dans quelle mesure, la personne concernée peut-elle prendre en charge sa protection au moment où la transparence des conséquences de ces décisions n'est pas assurée et où les choix n'existent pas toujours ? Ainsi, combien de sites ne refusent-ils pas l'accès aux utilisateurs qui n'acceptent pas les *cookies*? La négociation via le P3P risque elle-même d'être faussée lorsque le responsable du traitement propose insidieusement de « payer » l'obtention des données personnelles. Bref, comme l'écrit DIX[43] : « Technology is however no panacea for privacy risks in cyberespace ; it cannot replace a regulatory framework or legislation, contracts or code of conduct. Rather it may only operate within such a framework. Privacy by negotiation is therefore no alternative to regulation but a necessary additional tool ».

Sans doute, faut-il souligner à nouveau l'importance que pourrait apporter la participation des autorités de contrôle à la qualité de ces outils mis en place dans des cercles techniques ou des instances de normalisation dominés par les représentants des responsables de traitement[44].

[36] H. BURKERT, « Privacy Enhancing Technologies Typology, Critique, Vision », in P. AGRE et M. ROTENBERG (eds), *Technology and Privacy,* MIT Press, Cambridge, M.A., p. 125-143 ; L. LESSIG, *Code and other Laws of Cyberespace,* Basic Books, New York, 1999, p. 26 et s ; J. REIDENBERG, « Lex Informatica : the Formulation of Information Policy through Technology », 76 *Texas Law Rev.*, 1998, 552-593, Y. POULLET, « Technology and Law : from Challenge To Alliance », in *Information Quality Regulation : Foundations, Perspectives and Applications,* U. GASSER (ed.), Nomos Verlagsgesellschaft, 2004, Pour une présentation des PETs, voir le site de l'EPIC : http://www/epic.org/privacy/tools.html

[37] Y compris par les autorités de protection des données. Cfr. à cet égard le préambule de l'étude menée pour le Groupe de l'article 29 à cet égard : « Though technology can be used to invade our privacy, it also provides the far most effective means to protect it. Traditionally, technological data protection and privacy concepts are understood solely as security measures which are designed to ensure confidentiality and to restrict the availability of the data held. Encryption is in this sense one of the most effective tools. Though data security is still an important issue for the protection of privacy and personal data, awareness that it is even more important to keep the generation of personal data as such to a strict minimum is growing based on the simple fact that non-existing data cannot be misused. Where no personal data is needed, no personal data should be collected. When the collection of personal data is necessary for specific purposes, technology should be designed to enable the individual to use and pay for on-line services either in total anonymity or while using a pseudonym.
There are many tools for establishing this kind of privacy enhancing procedures, for example hash functions, digital signatures, biometric methods etc. At the moment, the most important thing is that society as a whole be informed about the risks to privacy that the use of information and communication technologies, in particular global networks such as the internet, present and of the concept and philosophy of data minimisation and « Privacy enhancing technology ». Consumers and legislators must demand and promote the use of privacy enhancing technology. Researchers and industry should integrate it at the earliest stage in designing information and communication technologies. » (http://europa.eu.int/comm/justice_home/fsj/privacy/studies/priv-enhancing_en.htm)

[38] À propos du P3P, lire J. CATLETT, *Technical Standards and Privacy : An open letter to P3P developers,* article disponible sur le site : http://www.junkblusters.com/standards.html

[39] Sur les différents protocoles d'encryptage et les serveurs d'anonymisation de même que sur les instruments d'anonymisation ou d'utilisation de pseudonymes, lire C.J. BENNETT et C.D. RAAB, *op. cit.*, p. 148 et s.

[40] Ainsi la liste noire mise en place par une société privée MAPS dont il faut bien reconnaître que l'intervention est bien plus efficace que les nombreuses interventions législatives des États à propos du spamming.

[41] À cet égard, les conclusions du projet PISA sur lequel nous reviendrons : « Privacy is probably more effective if transactions are performed by means of technologies that are privacy enhancing... rather than relying on legal protection and self-regulation. » (http ://dbs.cordis.lu/fep)

[42] Sur cette notion et le mythe qu'elle véhicule, M. D'UDECKEM- GEVERS et Y. POULLET, « Internet Content regulation : Concerns from a European User Empowerment perspective about Internet Content Regulation », *Communications & Strategies,* 2001, n° 43, p. 143-190.

[43] A. DIX, *Infomediaries and Negociated Privacy Techniques, papier présenté à la Conférence* « Computers, Freedom and Privacy » (CPF 2000), 19 avr., Toronto, disponible à : http://portal.acm.org/citation).

[44] Cf. la critique par le Groupe de travail de l'article 29 et celles de l'EPIC (Electronic Privacy Information Centre)(disponibles sur le site : http://www.epic.org/reports/prettypoorprivacy.html) à propos du P3P.

§ 2. L'INTERACTION ENTRE LES TROIS MODES DE RÉGULATION

Les considérations proposées ci-dessus envisagent de manière séparée les trois modes de régulation. Le propos de cette seconde section est d'approfondir les interactions entre les modes de régulation : celles que nous désignons, à la suite de l'accord interinstitutionnel européen sous le concept de « co-régulation ».

La conjonction des trois modes de régulation et leur bonne articulation constituent sans doute la bonne manière d'accroître la protection des personnes concernées[45]. L'exemple de *Privacy Policies* en témoigne. L'obligation légale de publier une page web relative à la pratique suivie en matière de protection des données, effectivement suivie par l'entreprise, accessible à l'utilisateur et conforme aux prescrits de la législation renvoie si on y regarde de près à quantité d'outils cette fois non nécessairement réglementaires. Les réalités et conformité de la pratique aux prescrits légaux peuvent être laissées à l'appréciation de certificateurs ou d'auditeurs[46] dont l'intervention sera démontrée par l'apposition d'un label. Les secteurs peuvent proposer des modèles de *Privacy Policies* pour éviter la disparité des formats, des modes d'expression et du vocabulaire utilisés. A défaut, peut-être faut-il prévoir une intervention législative[47] qui fixera ces divers points.

L'accessibilité de la *Privacy Policy* sera réalisée par des applications logicielles qui feront en sorte que la page constituera un passage obligé et, le cas échéant, autoriseront à un système expert de comparer les *Privacy preferences* de la personne concernée aux choix opérés par le responsable du traitement et relatés par la *Privacy Policy*.

[45] Sur ce point, lire J.R. REIDENBERG, « Privacy Protection and the Interdependence of Law, Technology and Self-regulation », in *Variations sur le droit de la société de l'information*, Cahier du Crid, n° 20, Bruylant Bruxelles, 2002, p. 126 et s.

[46] On peut concevoir que ces certificateurs et auditeurs soient eux-mêmes l'objet d'une accréditation selon un cahier des charges défini par une autorité publique ou en tout cas avec son aval. À ce propos, le système japonais du *Privacy Protection Mark* (PPM) décrit sur le site : http://www.privacymark.org. Ce système prévoit qu'une autorité, le JIPDEC, organe para public, examine le respect par les entreprises qui utilisent le PPM de leurs engagements et surtout la conformité de ces engagements avec les « MITI's Guidelines for Protection of Personal Information Related to Computer Processing in the Private Sector ». On ajoute qu' en 2000, JIPDEC annonçait son partenariat avec *BBBonline*, pur système d'autorégulation et affirmait le principe de la reconnaissance mutuelle des deux labels. Ainsi, la co-régulation à la japonaise déclare l'autorégulation américaine équivalente.

[47] Ainsi, huit institutions fédérales américaines ont lancé la procédure « d'Advanced Notice of Proposed Rulemaking » (ANPR) réclamant des commentaires publics à propos de l'amélioration des *Privacy Notices* que les institutions financières doivent fournir aux consommateurs dans le cadre du *Gramm-Leach-Billy Act*.

Un autre exemple est certes la régulation des labels de certification des sites web en matière de *privacy*[48]. La multiplication des labels induit la confusion de l'internaute. Quelle valeur accorder à un label susceptible d'être copié, émis en terre lointaine par un émetteur inconnu dont l'indépendance n'est pas évidente, dont la qualité du contrôle des sites est douteuse et peu armé lorsqu'il s'agit de sanctionner un non-respect aux règles du label. L' agréation des labels, c'est-à-dire le contrôle par une autorité publique ou par un organisme dont la composition atteste l'indépendance et la représentativité des divers intérêts, peut être une solution que les autorités publiques peuvent mettre en place ou initier[49].

Bref, les solutions sont à trouver, on le pressent, dans un *effective mix*, un système de co-régulation[50] où la loi trouve non seulement son prolongement mais également son effectivité dans des systèmes techniques et d'auto-réglementation qu'elle doit appeler de ses vœux et promouvoir.

Les limites de cet article obligent à restreindre l'étude de ce phénomène à ce que nous avons appelé la co-régulation descendante, c'est-à-dire les différentes hypothèses où la réglementation publique fait appel, promeut voire se réfère à des initiatives privées. Il eût été utile en effet d'aborder également la façon dont l'autorégulation spontanée peut susciter dans un second temps l'intervention réglementaire[51] (ce que nous qualifions d'autorégulation ascendante).

La co-régulation descendante part donc de l'intervention réglementaire et envisage la manière dont celle-ci tantôt suscite à l'appui de son initiative (I) le support d'autres modes de régulation, tantôt les reconnaît (II), tantôt les combat (III). Nos réflexions s'appuieront sur l'analyse de certaines dispositions des deux directives européennes en la matière.

[48] Sur la régulation des labels de certification, lire les recommandations de l'E-confidence Forum disponible sur le site : http://www.jrc.it

[49] Cfr. pour un tel mécanisme public-privé d'agréation des différents labels privés, mécanisme destiné à assurer la qualité des labels des sites web et leur respect des exigences des législations de protection des consommateurs et de sécurité, le système mis au point au Royaume Uni : TRUSTMARK UK. et le système mis au point au Japon sous l'égide du MITI.

[50] Sur la co-régulation, lire Y. POULLET, Technologies de l'information et de la communication et « co-régulation », une nouvelle approche ? *op. cit.*, p. 171. Cfr. également M. VIVANT, « Internet et modes de régulation », in *Internet face aux droits*, Cahier du Crid, n° 16, Kluwer, 199, p. 229 : « Au final, c'est bien de régulations au pluriel qu'il convient de parler, de modes de régulation qu'il convient d'articuler au mieux, de combiner en raison. ».

[51] À ce propos, on cite volontiers le cas canadien où la loi fédérale relative à la protection des données a entériné en ce qui concerne le secteur privé du moins le « modèle de code de conduite » développé par le comité de normalisation canadien.

A. L'autorégulation ou la technique à l'appui de la réglementation

L'article 27 de la directive 95/46/CE invite les États membres et la Commission « à encourager l'élaboration des codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales ».

Ainsi, est promue l'autorégulation qui se doit d'être conforme à la législation voire lui apporter une plus-value tant du point de vue de son contenu que de l'effectivité [52] [53].

On note également la possibilité laissée par l'article 18 de la directive aux responsables de traitement de nommer un « détaché » à la protection des données [54] et de bénéficier dès lors d'une dispense de notifier leurs traitements. A nouveau, le rôle de tels préposés est de relayer au sein de l'organe les préoccupations et exigences légales et de les traduire concrètement.

La même démarche de récompense [55] prévaut à propos de la procédure d'homologation des codes de conduite prévue à l'article 27.2. Il s'agit pour les auteurs du code de soumettre leurs textes à l'autorité de contrôle qui en vérifiera la conformité aux normes légales [56] : une telle homologation constitue, on le conçoit aisément, une présomption forte de conformité devant les tribunaux.

[52] Le cas hollandais où les codes de conduite sectoriels se sont multipliés doit être cité. A cet égard, lire G. OVERKLEEFT *Verburg, Wet persoonsregistraties: norm, toepassing en evaluatie*, Thèse, Tilburg, W.E.J., Tjeenk Wilrijk, 1995. Sur cet apport, ne serait-ce que par la lisibilité plus grande et l'application concrète de principes législatifs vagues à un cas concret, lire C.J. BENNETT et C.D. RAAB, « *The Governance of Privacy* », Ashgate, 2003, p. 122-123.

[53] Rien n'est dit par contre en ce qui concerne le besoin d'assurer une certaine légitimité aux codes de conduite ainsi par la nécessité d'une consultation des représentants des catégories des personnes concernées. Cette préoccupation au niveau européen de la légitimité des codes de conduite est exprimée pour la première fois en matière de protection des consommateurs par l'article 16 de la directive 2000/31/CE dite « Commerce électronique » du 8 juin 2000. On note cependant que le recueil des observations des personnes concernées est un élément de la procédure « d'homologation » prévue à l'article 27.2.

[54] Sur cette notion, son intérêt et les ambiguïtés réglementaires de la situation belge à ce propos, Y. POULLET, in *La sécurité informatique, entre technique et droit*, Cahier du Crid, n° 14, 1998, p. 215-217.

[55] Sur cette notion de « récompense », lire les réflexions de D.W.F. VERKADE, « De privacyfunctionnaris : geen zitjournalist, maar een doodgeboren kind ? », *Computerrecht*, 2001-2, p. 54.

[56] La même procédure existe au niveau européen. Le groupe de l'article 29 conformément à l'article 30, 1, de la Directive 95/46/CE approuve les codes de conduite communautaires. A noter l'application de cette procédure au code de conduite proposé par la FEDMA (Federation européenne de Direct Marketing) et approuvé par l'opinion 3/2003 du 13 juin 2003 disponible à l'adresse : http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77_fr.pdf

Deuxième exemple : la fixation de l'ampleur des mesures de sécurité à prendre par le responsable du traitement renvoie, selon l'article 17.1, à l'état de l'art, qui peut trouver expression dans des normes ou standards définis par des organes de normalisation [57].

B. La reconnaissance par la « loi » des autres modes de régulation

1. Les relations de travail

La régulation des relations de travail est souvent citée comme l'exemple type de « co-régulation ». La loi reconnaît en effet la portée obligatoire d'accords négociés dans un certain cadre par les prestataires sociaux. Ainsi, la Belgique prévoit le mécanisme de la Convention collective de travail et l'article 139 du traité de l'Union européenne, la vertu d'accords sociaux conclus à la suite de négociations menées sur une question de politique sociale [58].

C'est ainsi que se sont multipliées en Belgique les conventions collectives en matière de surveillance des employés [59].

Au plan européen, on note l'accord-cadre du 16 juillet 2002 relatif au télétravail, négocié et signé par les partenaires sociaux et dont un des objectifs principaux est certes la protection des données des travailleurs [60]. À ce propos, contrairement à l'approche belge qui permet la sanction par arrêté royal de la convention collective, les articles 138 et 139 du traité CE semblent exclure cette mise en œuvre par les autorités compétentes de l'Union européenne et laissent donc aux seules parties contractantes le soin de prévoir les moyens de l'effectivité de l'accord conclu.

[57] Cfr. à cet égard, les travaux récents du Comité européen de normalisation qui définissent des standards en matière de *Security and Privacy*. Sur ce même point, les nombreux exemples donnés par C.J. BENNETT et C.D. RAAB, *op. cit.*, p. 126 et s. et les réflexions de J. DUMORTIER et C. GOEMANS, « Online Data Privacy and Standardization : Towards amore effective Protection ? » in *A Decade of research @ the Crossroads of Law and ICT*, Larcier, 2001, p. 53 et s.

[58] Cfr. à ce propos, l'appel lancé aux partenaires sociaux pour qu'ils fassent usage de cette faculté dans le Livre Blanc sur la « Gouvernance européenne », COM (2001) 428 final, 25 juil. 2001, p. 18.

[59] À cet égard, en particulier la CCT n° 82 du 26 avr. 2002, conclue au sein du Conseil National du Travail relative à la protection des travailleurs à l'égard du contrôle des données de communications électroniques en réseau approuvée par l'Arrêté royal du 12 juin 2002 (*M.B.*, 29 juin 2002, p. 29486).

[60] Accord-cadre sur le télétravail disponible à l'adresse : http://europa.eu.int/comm/employment_social/news/2002/Jul/Telework_fi.pdf. Sur cet accord, M.V PEREZ-ASINARI, « L'accord cadre européen sur le télétravail, Aspects politiques et légaux. Un exemple de co-régulation ou d'autorégulation », *RDTI*, n° 15, 2003, p. 69.

Faut-il conclure que le texte laisse place à une pure autorégulation sanctionnée indirectement par le fait que les points de l'accord-cadre qui traite de la protection des données constituent sans doute une traduction *a priori* correcte des principes de la directive 95/46/CE[61] ? En définitive, l'accord-cadre européen est dans un premier temps à analyser comme la volonté des partenaires sociaux d'échapper à la réglementation publique par une régulation privée propre négociée entre représentants des deux parties intéressées : les travailleurs, d'une part ; les employeurs, d'autre part. Cette analyse semble devoir être remise en cause par la récente Communication de la Commission européenne[62] qui indique que lorsqu'un accord-cadre est conclu à une consultation lancée sur base de l'article 138 du Traité, la Commission non seulement se montrera attentive au suivi effectif de l'accord négocié par le contrôle de la réalisation des points de l'accord mais en outre peut étudier avec les partenaires sociaux les moyens nécessaires à cette effectivité. Il est difficile de ne pas voir dans cette Communication de la Commission une volonté de créer une plus grande synergie entre l'intervention publique certes subsidiaire et une réglementation privée qui n'est plus de ce fait abandonnée à elle-même mais trouve dans la mise à disposition par l'État de ses modes d'action une plus grande garantie d'effectivité.

2. Les flux transfrontières

Outre le domaine de la protection des données dans les relations employeurs-employés, la réglementation des flux transfrontières vers les pays extérieurs à l'Union européenne offre de beaux exemples de reconnaissance de modes privés de régulation.

Le principe de l'article 25 de la directive est, en cette dernière matière, l'interdiction des flux sauf si le pays destinataire offre une protection « adéquate ».

La notion, on l'a souligné par ailleurs[63], indique une approche souple et ouverte qui interdit à l'Europe d'imposer son modèle législatif de protection des données. Elle l'oblige à prendre en considération d'autres modèles de régulation et à rechercher si ceux-ci, fonctionnellement, garantissent effectivement les principes de protection des données. Sans doute, n'est-ce pas le lieu ici de détailler les *Safe Harbor Principles* américains, considérés comme offrant cette protection adéquate par la Commission européenne[64], mais de constater à cette occasion que l'Union européenne a reconnu qu'un objectif d'intérêt public comme la protection des données pouvait être atteint par un système de co-régulation dans un ordre juridique différent[65].

Cette « similarité fonctionnelle » d'un mode réglementaire étatique et d'un mode qu'il faut bien qualifier de co-régulation[66] est à souligner.

Le même raisonnement peut être poursuivi à propos des exceptions prévues par l'article 26, 2. L'article permet l'autorisation d'un transfert lorsque le responsable du traitement offre des « garanties suffisantes » au regard de la protection des données. Il ajoute que ces garanties peuvent notamment résulter de clauses contractuelles.

On connaît les « clauses contractuelles types » proposées par la Commission à cet égard[67]. Ainsi, l'autorégulation contractuelle certes encadrée

[61] Ainsi, on peut concevoir que la légitimité et la proportionnalité des traitements opérés par un employeur conformément à l'accord-cadre ne soient pas remises en cause en cas de contestation par un travailleur.

[62] Communication de la Commission, « *Le dialogue social européen, force de modernisation et de changement* », Proposition de Décision du conseil, COM (2002) 341 final, 26 juin 2002, p. 7.

[63] Sur cette notion de protection adéquate et les divers modes d'intervention de l'Union européenne en matière de flux transfrontières, Y. POULLET, Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données, *J. Cl. éd. Commerce électronique*, 2003, n° 12, p. 9 et s.

[64] Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the US Department of Commerce, *Official Journal* L 215/7 of 25.8.2000.

[65] Pour un exposé complet en la matière, le lecteur se référera aux articles suivants : B. HAVELANGE et A.-C. LACOSTE, Les flux transfrontières de données à caractère personnel en droit européen, *JTDE*, 2001, p. 240 et s. ; Y. POULLET , S. LOUVEAUX & M.V. PEREZ- ASINARI, « Data Protection and Privacy in Global networks : A European Approach », *EDI Law Review* 8, 147-196, 2001 ; P.M. SCHWARTZ, « European Data Protection Law and Restriction on International Data Flows, 80 » *Iowa Law Rev.*, 1995, n° 3, p. 473 et s. ; J.R. REIDENBERG, « E-commerce and Trans-Atlantic Privacy, 38 », *Houston Law Rev.*, (2001), 3, p. 719 et s.

[66] L'action des pouvoirs publics dans l'encadrement de la régulation privée interdit en effet de voir dans *les Safe Harbor Principles* une pure autorégulation. On sait l'importance qu'a eu l'initiative gouvernementale américaine dans l'écriture des principes et la négociation de leur caractère adéquat avec la Commission, on note que les déclarations des entreprises en ce qui concerne le respect des *Principles* et leur *Privacy Policy* s'opèrent auprès du *department of Commerce*? Enfin, on souligne l'importance qu'a prise aux yeux de la Commission dans l'appréciation du caractère adéquat la possibilité de recours de la personne concernée auprès de la juridiction administrative : *la Federal, Trade Commission FTC*), en cas de non-respect par une entreprise des principes du *Safe Harbor*. La législation punit en effet *le Deceiptive or False Statement*, et ouvre au consommateur victime une action facile et peu coûteuse devant la F.T.C. Tout ce contexte réglementaire donne à la déclaration relative à la *Privacy Policy* d'une entreprise américaine toute sa valeur juridique et en garantit l'effectivité.

[67] Décision de la Commission 2001/497/CE du 15 juin 2001, *J.O.* L 181/19 du 4 juil. 2001 à propos des clauses contractuelles relatives à des transferts de données vers des responsables de données établis dans des pays tiers. Décision de la Commission 2002/16/CE du 27 déc. 2002,

réglementairement par quelques règles dérogatoires au droit commun [68] peut également offrir la protection fonctionnellement similaire réclamée par la directive.

Mieux, une opinion récente du Groupe dit de l'article 29 estime que cette protection similaire peut être offerte par la *Privacy Policy* d'une multinationale à condition qu'elle réponde à certaines conditions [69]. On s'interroge donc sur la portée d'un règlement interne à une multinationale, ce que le Groupe dit de l'article 29 qualifie de *Binding Corporate Rules.* Quelle valeur reconnaître à un document par lequel un groupe régule ses flux internes ? À l'inverse des règles professionnelles ou de codes de conduite sectoriels, l'autorégulation n'est pas ici imposée de l'extérieur de l'entreprise ou à son groupe, elle est générée en leur sein sous forme d'une charte, d'un code de conduite d'une *Privacy Policy* du groupe ou d'un règlement édicté par la maison mère [70]. Pour reconnaître le caractère contraignant de telles règles, le document de travail distingue le plan du droit (le caractère juridiquement exécutoire) et le plan pratique pour affirmer tout de suite que si le caractère contraignant doit être apprécié sur les deux plans, le second plan est important dans une configuration transfrontalière où la reconnaissance des droits s'avère difficile et où « il importe (dès lors) non seulement de veiller à ce que les règles internes soient exécutoires d'un point de vue juridique mais également d'un point de vue pratique ».

J.O. du 10 janv. 2002 à propos des clauses contractuelles types pour le transfert de données vers des sous-traitants établis dans des pays tiers. Cfr. également l'avis 8/2003 du groupe dit de l'article 29 du 17 sept. 2003 relatif au projet de clauses contractuelles types présentées par un groupe d'associations professionnelles. Sur ces décisions et l'avis, voir le site de la Commission européenne en matière de protection des données : http://europa.eu.int/comm/justice_home/fsj/privacy/

[68] On ôte ainsi sans être exhaustif la clause de stipulation pour autrui au profit de la personne concernée, les clauses relatives à la responsabilité solidaire (dans les deux premières décisions de la Commission) de l'importateur et de l'exportateur en cas de violation des engagements contractuels, la clause relative au droit applicable, etc.

[69] Groupe de travail art.29, « Transferts de données personnelles vers des pays tiers : application de l'article 26 (2) de la Directive de l'U.E relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données », W.P.74, adopté le 3 juin 2003. Sur ce document nos commentaires in » Flux transfrontières de données, Vie privée et groupes d'entreprises : À propos d'une opinion récente du groupe de travail de l'article 29 et d'une décision récente de la Commission belge de protection des données, *RTDI*, 2005, à paraître. Cfr. depuis, les deux documents du 14 avril, d'une part, mettant en place la procédure de coopération entre autorités de protection des données à propos des règles contraignantes et, d'autre part, fixant *la check list* modèle de telles règles.

[70] Cfr. à ce propos, la typologie *ratione personae* proposée par J. BERLEUR et T. EWBANK à propos des documents d'autorégulation, in Gouvernance de l'Internet : Réglementation, autorégulation, co-régulation ?, in *Gouvernance de la Société de l'Information*, Cahier du CRID n° 20, Bruylant, Bruxelles, 2002, p. 34 et s.

On sait que l'unité économique que peut représenter un groupe de sociétés ne se conçoit pas sans une structure hiérarchique forte et des moyens de contrôle importants du respect des décisions prises à la tête du groupe [71]. La structure interne du groupe donne donc aux décisions d'autoréglementation prises en son sein et au plus haut niveau une force évidente mais, dans le même laps de temps, il faut bien reconnaître que dans le domaine qui est celui de la protection des données, l'intérêt poursuivi n'est pas nécessairement l'intérêt économique du groupe même si la bonne gestion des données nominatives peut contribuer à la bonne image du groupe. En d'autres termes, il n'est pas toujours évident que la règle, le code de conduite ou la *Privacy Policy* décidés au sein du groupe fassent l'objet d'une attention particulière de la hiérarchie du groupe, s'il n'y a pas menace de contraintes cette fois juridiques, forçant la hiérarchie à utiliser les moyens de pression et de contrainte internes au groupe.

On conçoit dès lors que le Groupe 29 ait exigé explicitement une nature contraignante des règles tant en droit qu'en pratique et souligner le caractère complémentaire de cette double contrainte même si le document souligne le caractère prépondérant de la contrainte non juridique « Si la possibilité pour les personnes concernées de faire respecter les règles en recourant à la justice constitue un élément nécessaire pour les raisons qui viennent d'être exposées, le groupe de travail « Article 29 » attache encore plus d'importance à l'application pratique de ces règles par le Groupe dans la mesure où il s'agit là de la finalité de toute approche fondée sur l'autoréglementation [72] ». En d'autres termes, c'est dire combien l'« effectivité » de l'auto-réglementation est considérée comme un élément central de sa validité.

C. Le contrôle voire le rejet des autres modes de régulation

Les réflexions menées sous le point B montrent bien que la reconnaissance par les textes européens des autres modes de régulation de la protection des données s'accompagne d'un contrôle ou tout au moins d'un cer-

[71] On pourrait difficilement accepter que les règles d'entreprise ne soient pas adoptées ou en tout cas explicitement avalisées par le sommet de la hiérarchie, par exemple par le Conseil d'administration de la maison mère du groupe. Quelle valeur pourrait être accordée à la déclaration d'un simple administrateur de filiale voire d'un président des implantations européennes du groupe, s'il n'y a pas d'une manière explicite une « couverture » de tels engagements par la maison mère ?

[72] Document de travail n° 74, *déjà cité*, p. 12.

tain encadrement de ces derniers. Ainsi, la reconnaissance par l'autorité du caractère adéquat offert par un système juridique différent de celui européen et fondé sur l'autorégulation exige une analyse sévère du respect des critères développés par l'autorité publique. La technique des clauses types contractuelles permet de suggérer aux acteurs privés un modèle de référence soit qu'ils reprennent soit dont ils sont invités à ne pas trop s'écarter. La façon dont les *Binding Corporate Rules* sont soumises à diverses exigences pour constituer « des garanties suffisantes et appropriées » de protection des données a été soulignée.

De même à l'occasion de l'homologation des codes de conduite, les autorités de protection des données sont-elles sensibles à un examen serré des conditions de conformité du contenu de la protection offerte par l'instrument aux exigences de la loi de protection des données, à la légitimité de leurs auteurs et, enfin, à l'effectivité plus grande offerte par ces modes de régulation à l'appui de la protection déjà inscrite dans les législations de vie privée.

Notre propos est, au delà de ce contrôle par le droit des autres modes de régulation, son rejet de certaines technologies dont le fonctionnement est, selon l'expression de Jean-Marc DINANT[73], « privaticide ». Deux dispositions de la directive 2002/58/CE relative à la protection des données dans les secteurs des communications électroniques illustrent notre propos.

L'article 5, 3 conditionne « l'utilisation des réseaux en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ». On connaît cette pratique des *cookies*[74], *spywares* ou logiciels espions introduits dans le terminal de l'utilisateur et qui permettent tantôt de prendre le contrôle à distance de l'utilisateur, tantôt de connaître les éléments stockés sur celui-ci[75], tantôt enfin de mettre à jour des logiciels acquis par l'internaute sans que celui-ci n'ait nécessairement conscience de cette mise à jour[76]. Sans entrer dans le détail du prescrit, notons l'obligation d'informer l'internaute de cette intrusion possible et de

[73] J.-M. DINANT, « Les traitements invisibles sur Internet », in *Droit des technologies de l'information et de la communication : regards prospectifs* ,Cahier du Crid, n° 16, p. 271 et s.

[74] Sur ces différentes technologies, lire la recommandation 1/99 du groupe dit de l'article 29 sur le traitement invisible et automatique des données à caractère personnel sur l' Internet effectué par des moyens logiciels et matériels, 23 févr. 1999, W.P.17, Doc 5093/98.

[75] On citera le cas du logiciel espion inséré dans le service « Real Jukebox » proposé par la société *Real Networks*, société permettant l'accès et le télé déchargement de musique en ligne. À travers le télé déchargement des musiques, le service introduisait dans le terminal de l'utilisateur un logiciel permettant de détecter des copies illicites.

[76] De nombreux fournisseurs (Microsoft, Intel, etc. par ex.) procèdent ainsi.

ses finalités de même que le droit de celui-ci de refuser l'intrusion. En d'autres termes, la loi refuse certaines régulations technologiques et oblige le producteur de tels produits à définir les spécificités de son produit ou service à certaines exigences légales.

L'article 14 peut être analysé de la même manière. Après avoir affirmé le principe du libre accès au marché des équipements terminaux et prohiber toute « exigence quant aux caractéristiques de ces terminaux », il réserve la possibilité pour la Commission d'imposer des spécifications techniques à ces produits de telle manière qu'ils soient « construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel ». Des normes techniques[77] peuvent être établies à cet effet. Elles tendent à assurer que le fonctionnement des équipements terminaux soit en conformité avec les exigences réglementaires[78].

Une telle tendance de la loi d'inscrire l'exigence de son respect au cœur du fonctionnement technologique est remarquable. Il est évident que « la normativité (voulue par la loi) est tributaire de la technique »[79]. Le critère de « conformité » rappelé dès l'introduction exige que les modes de régulation normatifs non juridiques présentent des solutions au contenu en accord avec la régulation juridique : comment ne pas dès lors comprendre ce souci du législateur de ne pas vider de sens la protection légale qu'il institue par le développement de technologies dont l'effectivité bien plus grande que celle de la loi pourrait dans les faits rendre creuses les dispositions légales ? Exprimée autrement et positivement cette fois, comment la loi pourrait-elle se priver de l'appui de la technologie pour obtenir sa pleine effectivité[80] ?

[77] Sur le rôle de la standardisation comme outil de régulation technique capable d'assurer le respect des prescrits légaux et la critique des processus actuels de standardisation, lire *le Discussion Paper* récemment établi par le *ICT Standards Board, Critical Issues in ICT Standardization*, 27 avr. 2005 (disponible sur le site : http://www.ictsb.org)

[78] Sur ce besoin de la technologie de se conformer dans son design aux exigences de la protection voulue par la loi, lire J.R. REIDENBERG, « Privacy Protection and the Interdependance of Law, Technology and Self-Regulation », in *Variations sur le droit de la société de l'information*, Cahier du Crid, n° 20, Bruxelles, Bruylant, 2002, p. 138.

[79] E. LABBÉ, « La technique dans la sphère de la normativité : aperçu d' un mode de régulation autonome », *Juriscom.net*, novembre 2000, disponible sur le site : http://www.juriscom.net/uni/doc/20001108.htm.

[80] Sur ces différents points, lire T. SCHULTZ, *op.cit.* On évoquera à ce propos la volonté des autorités publiques de développer les PETS (*Privacy Enhancing Technology Systems*) voire à les rendre obligatoires. Sur les PETS et leurs différentes catégories, voir nos réflexions *supra*.

CONCLUSIONS

La régulation de l'Internet ne peut reposer ni sur le seul acteur que constitue l'autorité publique, ni sur le seul mode de régulation que constitue la norme juridique. Notre objectif était de montrer que seule une approche internormative peut apporter aux citoyens la protection de ses données à caractère personnel. Cette nécessaire ouverture du Droit aux autres modes de régulation et le dialogue que le Droit doit entretenir avec les acteurs de ces modes alternatifs de régulation que sont les associations professionnelles, les industries du logiciel et des terminaux conduisent à prôner à la fois humilité et fermeté aux autorités publiques.

Humilité, dans la mesure où le Droit et le juriste doivent quitter les cercles restreints où s'élabore traditionnellement la loi entendue au sens le plus large pour pénétrer les milieux où s'élaborent l'autorégulation et la régulation technique. Le juriste doit apprendre en particulier à discuter des solutions technologiques et dialoguer avec les milieux professionnels [81] ne serait-ce que pour trouver sur le marché même des alliés [82] aptes à offrir des solutions qui prolongeront par leurs services la protection que le Droit souhaite offrir.

Fermeté, dans la mesure où comme le rappelait le document « Mieux légiférer » de l'Union européenne, les mécanismes de régulation alternatifs ne peuvent être appliqués « si les droits fondamentaux ou des choix politiques importants sont en jeu ». C'est aux autorités publiques de fixer les lignes essentielles des protections indispensables à la garantie des libertés des citoyens. Elles veilleront à fixer le cadre protecteur de manière technologiquement neutre et conformément aux principes de subsidiarité [83] et de

[81] « Privacy protection must be negociated through the system described in the figure and is not necessarily commanded from the top, especially as in the view of some governance and network theories there may be non identifiable top except in formal and procedural terms. The role of the State cannot be overlooked, but the exercise of constitutional authority may not be prevalent in particular situations. » (C.J. BENNETT ET C.D. RAAB, *op. cit.*, p. 175).

[82] À cet égard, le rôle que pourraient jouer de nouveaux acteurs, tels les infomédiaires qui, interfaces entre l'internaute et les fournisseurs de services de la société de l'information, pourraient offrir aux premiers des services de protection de leurs données (filtrage des communications non sollicitées, service d'anonymisation, gestion des cookies, etc.). Sur ce nouveau marché, lire l'excellent article de P. TABATONI, « Stratégies de la Privacy aux États-Unis : la dynamique des systèmes de protection », in *Groupe d'études Société de l'information et vie privée*, p. 220 et s. texte disponible sur le site : http://www.asmp.fr

[83] « 16. Les trois institutions rappellent que la Communauté (européenne) ne légifère que dans la mesure nécessaire, conformément au protocole sur l'application des principes de subsidiarité et de proportionnalité. Elles reconnaissent l'utilité de recourir, dans les cas appropriés, à des mécanismes de régulations alternatifs » (Point 16 de l'accord institutionnel cité note 82).

proportionnalité. Il ne s'agit pas pour elle de trop dire, ni *a fortiori* de tout dire mais de laisser à d'autres modes de régulation ainsi encadrés le soin de répondre de manière appropriée aux objectifs qu'elle aura fixés et vis-à-vis desquels les pouvoirs privés, auteurs des normes techniques ou d'autorégulation, devront se conformer.